Lecture 3.

Rings.

Def. A **ring** is a set R with two binary operations $+$ and $\cdot$ such that

1) $(R, +)$ is an abelian group;

2) the operation $\cdot$ is associative, i.e.

$(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \forall a, b, c \in R$;

3) the distributivity laws hold:

$$a \cdot (b + c) = a \cdot b + a \cdot c, \quad (b + c) \cdot a = b \cdot a + c \cdot a$$

$\forall a, b, c \in R$.

Examples: $\mathbb{Z}$, $\mathbb{Z}(n)$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$

Let $M_n(\mathbb{R})$ be the set of $n \times n$ matrices over $\mathbb{R}$ with matrix addition and multiplication. Then $M_n(\mathbb{R})$ is a ring.

An element $1 \in R$ is called an identity if

$a \cdot 1 = 1 \cdot a = a \quad \forall a \in R$.

we don't include existence of such elements in the definition of a ring.

Subrings.

A subset $S \subset R$ of a ring R is called a subring if $\forall a, b \in S$ $a+b, a-b, a \cdot b$ again lie in S. Then S can be considered as a ring on its own.

Examples. $\mathbb{Z} < \mathbb{Q} < \mathbb{R} < \mathbb{C}$,

$n\mathbb{Z} < \mathbb{Z}$.

Def. A subring $S \subset R$ is called an ideal if $\forall a \in S \ \forall x \in R$ $ax, xa \in S$.

Example. $n\mathbb{Z}$ is an ideal of $\mathbb{Z}$.

Notation: if I is an ideal of R then we write $I \trianglelefteq R$.

(0) and R are always ideals of a ring R. They are referred to as trivial ideals.

A nontrivial ideal is an ideal that is different from (0) and R.

If 1 is the identity of a ring R and $I \trianglelefteq R$ then $1 \in I$ implies $I = R$.

Rings $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_{(p)}$ do not contain any nontrivial ideals because we can divide by nonzero elements. If $I \trianglelefteq R$, $0 \neq a \in I$ then for an arbitrary element $x \in R$ we have

$x = a \cdot \left(\frac{x}{a}\right) \in I$, so $I = \mathbb{Q}$.

Exercise. Nontrivial ideals of a ring $\mathbb{Z}(n)$, $n \geq 2$, are $m\mathbb{Z}(n)$, $\gcd(m,n) \neq 1$, $n \nmid m$.

Isomorphisms.

Let R, S be rings. A mapping $\varphi : R \to S$ is called an isomorphism if

(1) φ is a bijection;

(2.1) $\varphi(a \pm b) = \varphi(a) \pm \varphi(b)$ $\forall a, b \in R$ (φ preserves addition);

(2.2.) $\varphi(ab) = \varphi(a)\varphi(b)$ $\forall a, b \in R$ (φ preserves multiplication).

As in the case of groups if $\varphi : R \to S$ is an isomorphism then $\varphi^{-1} : S \to R$ is also an

isomorphism.

We do not distinguish between isomorphic rings.

Example. $\mathbb{R}$ is a subring of $M_2(\mathbb{R})$.

Indeed, consider the subring

$$S = \left\{ \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix}, \alpha \in \mathbb{R} \right\} < M_2(\mathbb{R}).$$

The mapping $\varphi : \mathbb{R} \to S$, $\alpha \to \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix}$, is an isomorphism. We don't distinguish between $\mathbb{R}$ and S. Hence $\mathbb{R} < M_2(R)$.

Homomorphisms.

Def. A mapping $\varphi : R \to S$ is called a homomorphism if (2.1) and (2.2) hold, i.e. φ preserves both operations:

addition and multiplication.

Example. $\varphi : \mathbb{Z} \to \mathbb{Z}(n)$,

$a \to$ remainder of $a \bmod n$, is a homomorphism.

Example. The mapping $\varphi : \mathbb{R} \to M_2(\mathbb{R})$,

$\alpha \xrightarrow{\varphi} \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix}$, is a homomorphism.

Question: is any of the examples above an isomorphism?

Example. Let $m, n \geq 2$, $m \mid n$. Then the mapping $\varphi : \mathbb{Z}(n) \to \mathbb{Z}(m)$,

$a \to$ remainder of $a \bmod m$, is a homomorphism.

Question: is the mapping $\mathbb{Z} \to 2\mathbb{Z}$, $a \to 2a$, a homomorphism?

Let R, S be rings and let $\varphi: R \to S$ be a homomorphism. The subset

$$\operatorname{Ker}\varphi = \{a \in R \mid \varphi(a) = 0\}$$

is called the <u>kernel</u> of the homomorphism φ.

<u>Lemma.</u> $\operatorname{Ker}\varphi \trianglelefteq R$.

<u>Proof.</u> Let $a, b \in \operatorname{Ker}\varphi$. Then

$$\varphi(a \pm b) = \varphi(a) \pm \varphi(b) = 0 \pm 0 = 0.$$

Hence $a \pm b \in \operatorname{Ker}\varphi$.

Let $x \in R$. Then $\varphi(ax) = \varphi(a)\varphi(x) =$

$0 \cdot \varphi(x) = 0$ and, similarly, $\varphi(xa) =$

$\varphi(x)\varphi(a) = \varphi(x) \cdot 0 = 0$.

We proved that $\operatorname{Ker}\varphi$ is an ideal of R. $\blacksquare$

Example. Consider the homomorphism

$\varphi: \mathbb{Z} \to \mathbb{Z}(n)$, $a \to$ remainder of a mod n.

What is $\ker\varphi$? The $\ker\varphi$ is $n\mathbb{Z}$.

The kernel of an isomorphism is (0) because an isomorphism is a bijection.

Factor - Rings.

Let R be a ring and let I be an ideal of the ring R.

The set R with the operation $+$ is called the additive group of R (we "forget" about multiplication): $(R,+)$.

$(R,+)$ is an abelian group, I is a subgroup of $(R,+)$.

Cosets of I = cosets of the subgroup I in $(R,+) = \{a+I\}$.

Here $a+I = \{a+b,\ b \in I\}$.

Example. $R = \mathbb{Z}$, $I = 5\mathbb{Z}$.

Cosets: $5\mathbb{Z}$, $1+5\mathbb{Z}$, $2+5\mathbb{Z}$, $3+5\mathbb{Z}$, $4+5\mathbb{Z}$.

Cosets correspond to remainders mod 5.

Every element from a coset completely determines the coset. Let $a, b \in R$ lie in the same coset. It means that

$$a - b \in I.$$

Then $a+I = b+I$. Indeed, choose an element $a+x \in a+I$, $x \in I$. Then

$a+x = b+\underbrace{(a-b)+x)}_{\in I} \in b+I$. Hence

$a+I \subseteq b+I$ and similarly $b+I \subseteq a+I$.

Let R/I = the set of all cosets of I.

we will define addition and multiplication on the set R/I.

Given two cosets $a+I$ and $b+I$ we define

$(a+I)+(b+I) = a+b+I$.

Question: is it well defined?

Choose another element a' from the coset $a+I$ and another element b' from $b+I$. Then

$a+I = a'+I$, $b+I = b'+I$, $(a'+I)+(b'+I) = a'+b'+I$.

Are we sure that $a+b+I = a'+b'+I$?

Yes we are: $a+b$ and $a'+b'$ lie in the same coset. Since a and a' lie in the same coset it follows that $a-a' \in I$. Since b and b' lie in the same coset it follows that $b-b' \in I$. Now $(a+b)-(a'+b') = (a-a')+(b-b') \in I$.

Thus the addition is well defined.

Given two cosets $a+I$ and $b+I$ we define

$$(a+I)(b+I) = ab+I.$$

Is it well defined?

Again, let $a+I = a'+I$, $a-a' \in I$.

Let $b+I = b'+I$, $b-b' \in I$.

Then $(a'+I)(b'+I) = a'b'+I$.

We need to show that

$$ab+I = a'b'+I,$$

that is, $ab - a'b' \in I$.

We have

$$ab - a'b' = ab - ab' + ab' - a'b' =$$

$$= a\underbrace{(b-b')}_{\in I} + \underbrace{(a-a')}_{\in I}b' \in I.$$

Thus the multiplication is well defined.

Now the set R/I is equipped with two binary operations: addition and multiplication.

The axioms of a ring are inherited from the ring R.

For example, let us check associativity of the multiplication.

$$\big((a+I)(b+I)\big)(c+I) \stackrel{?}{=} (a+I)\big((b+I)(c+I)\big)$$

The left hand side $= (ab+I)(c+I) = (ab)c + I$.

The right hand side $= (a+I)(bc+I) = a(bc) + I$.

But $(ab)c = a(bc)$.

Def. The ring R/I is called the factor ring of R modulo I.

First Theorem about homomorphisms.

Let $\varphi: R \to S$ be a surjective homomorphism of rings (that is, $\varphi(R) = S$).

Let $I = \ker \varphi$. Then $R/I \cong S$.

Proof. Let's define a mapping

$$\psi : R/I \to S.$$

Given a coset $a+I$ we let

$$\psi(a+I) = \varphi(a).$$

Is it well defined?

Let $a+I = a'+I$, so $a-a' \in I$.

We need to show that $\varphi(a) = \varphi(a')$.

But $\varphi(a) - \varphi(a') = \varphi(a-a') = 0$ since

$a-a' \in I = \ker \varphi$.

Thus the mapping ψ is well defined. We will show that ψ is an isomorphism.

(1) Bijection. The mapping ψ is surjective because φ is surjective.

why is it injective?

Let $\Psi(a+I) = \Psi(b+I)$. We need to show that $a+I = b+I$.

$\Psi(a+I) = \varphi(a)$, $\Psi(b+I) = \varphi(b)$, hence

$$\varphi(a) = \varphi(b), \quad \varphi(a) - \varphi(b) = 0,$$

$$\varphi(a-b) = 0.$$

We showed that $a-b \in \operatorname{Ker}\varphi = I$. This implies that $a+I = b+I$.

(2) Operations.

$$\Psi\big((a+I)+(b+I)\big) = \Psi(a+b+I) = \varphi(a+b)$$

$$\Psi(a+I) + \Psi(b+I) = \varphi(a) + \varphi(b).$$

Hence,

$$\Psi\big((a+I)+(b+I)\big) = \Psi(a+I) + \Psi(b+I),$$

Ψ preserves addition.

Similarly,

$$\psi\left((a+I)(b+I)\right) = \psi(ab+I) = \varphi(ab),$$

$$\psi(a+I)\,\psi(b+I) = \varphi(a)\,\varphi(b),$$

$$\psi\left((a+I)(b+I)\right) = \psi(a+I)\,\psi(b+I).$$

we proved that ψ preserves multiplication. ∎

Example. $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}(n)$.

Indeed, the homomorphism $\mathbb{Z} \xrightarrow{\varphi} \mathbb{Z}(n)$ is surjective and $\ker \varphi = n\mathbb{Z}$.

Example. Consider the homomorphism

$$\mathbb{Z}(12) \xrightarrow{\varphi} \mathbb{Z}(4)$$

$$a \to \text{remainder of } a \bmod 4.$$

$\ker \varphi = 4\,\mathbb{Z}(12) = \{0, 4, 8\}$. Hence

$$\mathbb{Z}(12)/4\,\mathbb{Z}(12) \cong \mathbb{Z}(4).$$